State of South Carolina – Human Resources Division

InfoSec / Privacy Workforce

Technical Interview Questions

Risk Management and Compliance Technical Interview Questions by Position Description

Contents

Introduction & Guidelines

The Information Security (InfoSec) and Privacy Technical Interview Questions were created for each InfoSec and Privacy Position Description to support the hiring of personnel, where appropriate. These questions can be used when interviewing for core InfoSec and Privacy positions, and take into account position-related knowledge, experience, and proficiencies. Please note the following guidelines when using the Technical Interview Questions:

- These questions are **suggestions for topics that could be discussed** during the interview process of potential questions. They **should not be used as a stand-alone** guide when preparing to interview a candidate
- The guide is **not a replacement but a supplement** for the questions used to screen candidates for the expertise and skills that are required for the position.
- This list of questions is **not all encompassing** and only **consists of a sample set** of potential questions
- The questions have been prepared with the expectation that the interviewers fully-understand the topics that are discussed. There is **no answer key** to guide the interviewers for the questions in this guide
- Recommendations for the interview process **may consist of team of members** in relationship to the roles and responsibilities for the position being hired, leadership positions, as well as a consumer, stakeholder, or customer of the organization.
- These questions are based on **current Position Description needs**. They are **subject to revision** based on new requirements as deemed necessary by DIS, EPO, and/or DSHR
- **Please contact the InfoSec & Privacy PDP Program Manager or your HR Consultant should you have any other questions** regarding the usage of the technical interview questions in this document

Information Privacy Analyst

Level I, II, and III

- What is the key function/mission of a privacy office?
- What are some common information privacy risks related to the storage and sharing of information technology data?
- Describe the importance of data classification.
- How do you apply/operationalize a data classification schema?
- Describe the major components and steps in a privacy incident response process.
- What are the latest information privacy threats you foresee in the near future?
- Describe your experience with the data lifecycle. What are key components of the data lifecycle (e.g., identification, use, access, transmission, storage and destruction of data) and how have you employed them?

Level II and Above

- What are some federal privacy laws that would be applicable to the State? How do you keep up with changes to these laws?

Level III Only

- Describe pervasive privacy risks applicable to this agency and how to minimize them.

Information Privacy Manager

Level I, II, and III

- What are some federal privacy laws that would be applicable to the State? How do you keep up with changes to these laws?
- Describe your knowledge of information privacy laws, policies, procedures, and technologies.
- Describe the importance of data classification.
- How do you apply/operationalize a data classification schema?
- What is your experience in developing and managing a privacy program? What policies, training, standards, procedures, technologies (e.g., system and network security, encryption, and authentication) and controls did you employ?
- What does the ideal privacy program look like (e.g., structure, governance, executive sponsorship, and training)? How do you prioritize and delegate responsibilities in developing this program? Describe the steps you would take to implement this program.
- Describe your experience with the data lifecycle. What are key components of the data lifecycle (e.g., identification, use, access, transmission, storage and destruction of data) and how have you employed them?
- Describe your experience performing privacy risk assessments.
- What would be the ideal privacy incident response process for the State?
- Describe pervasive privacy risks applicable to this agency and how to minimize them.
- What are the latest information privacy threats you foresee for the near future?
- How do you tailor program communications to different audiences (e.g., technical, non-technical, across organization levels)?

Information Security Analyst

Level I, II, and III

- What is your experience with data collection, transmission, and storage methods as it relates to information security?
- Describe your technical expertise in the operation or management of operating systems, networks & infrastructure, and application platforms.
- What are some of the current vulnerability trends when it comes to IT infrastructure (e.g., networks, servers) and how can these be addressed?
- Describe the objective, process, and outcome of an information security risk assessment project.
- What is your understanding of a layered security approach?
- What are some of the technologies uses to minimize risks of:
    - Data confidentiality breach
    - Data integrity
    - Data availability

Level II and Above

- What is your experience in the installation, setup, and operation of IT infrastructure (e.g., routers, switches, firewalls, data encryption, and intrusion protection devices)?
- Describe the importance of implementing a baseline configuration for firewalls. What are some of the key risks of not having one?
- What is the difference between symmetric and asymmetric encryption? Explain how asymmetric encryption works.
- Explain how the Secure Socket Layer (SSL) protocol works.
- Describe your experience performing vulnerability assessments; including scanning, analysis of results, and manual validation? Are there methods of obscuring a port scan?
- Describe the ideal incident response process.
- What are the most common application security flaws?
- What are some federal information security laws that would be applicable to the State? How do you keep up with changes to these policies?
- Describe the importance of having a controls framework.

Level III Only

- Describe some possible vulnerabilities in the implementation of SSL.
- What is a plan of actions & milestones (PO&AM)? Why is important to have one?

Information Security Architect

Level I, II, and III

- How familiar are you with information security principles (e.g. confidentiality, integrity and availability)? Do you have any experience applying these principles in practice?
- Please indicate your experience in using or managing information security technologies related to:
    - Access control and multi-factor authentication
    - Encryption of data at rest and in transit
    - Network Security
- What is the difference between symmetric and asymmetric encryption? Explain how asymmetric encryption works.
- What is your understanding of a layered security approach?
- What are the distinctions between business information systems and technology architecture layers? What are some dependencies that exist between the two?
- Explain how the Secure Socket Layer (SSL) protocol works.
- Why should I use server certificates on my e-commerce website?
- What kind of authentication does Active Directory (AD) use?
- What is your experience performing and analyzing results of network/infrastructure and applications vulnerability assessments and penetration tests?
- What is a stateful packet inspection?
- Your network has been infected by malware. Please walk me through your mitigation process at a high level.
- What is a Syn Flood attack, and how can it be prevented?
- What is Cross-Site Scripting and how can it be prevented?
- What is a Man-in-the-Middle attack and how can it be prevented?
- Can a server certificate prevent SQL injection attacks against your system? Please explain.
- Describe an experience where you managed or responded to an information security threat or incident. What was the outcome?
- Describe your technical proficiency in information technology. What is your experience with operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), servers, cloud computing, networks, desktops, and mobile devices?
- What are some federal information security laws that would be applicable to the State? How do you keep up with changes to these laws?

Level II and Above

- What are some new developments in next generation firewall technologies (NGFW)?
- Describe the process to perform a network vulnerability assessment, How would you prioritize resolution of vulnerabilities found?
- How would you harden a server (e.g. Windows, Linux, etc.)?
- Are you aware of recent vulnerabilities in the implementation of SSL?

Level III Only

- What is your experience developing executive reports based on findings for presentation to leadership?
- What is your experience developing plan of actions & milestones (PO&AM) and tracking progress?

Information Security Engineer

Level I, II, and III

- How familiar are you with information security principles (e.g. confidentiality, integrity and availability)? Do you have any experience applying these principles in practice?
- What is your knowledge of networking protocols and information security related technologies (e.g. encryption, firewalls, antivirus software, intrusion prevention systems, and access lists)?
- What is your understanding of a layered security approach?
- What is the difference between a proxy and a firewall? What is the better approach setting up a firewall: dropping or rejecting unwanted packets and why?
- What is the difference between symmetric and asymmetric encryption? Explain how asymmetric encryption works.
- What is the difference between encryption and hashing?
- What is your experience in information security incident response?
- Describe your knowledge of programming code, scripting and concepts.
- What is the difference between penetration testing and vulnerability scanning?
- What is your experience in performing and managing vulnerability assessments and penetration tests on network infrastructure and applications? What kind of security testing and penetration testing tools have you employed?
- Your network has been infected by malware. Please walk me through your mitigation process at a high level.
- What is a Syn Flood attack, and how can it be prevented?
- What is Cross-Site Scripting and how can it be prevented?
- What is a Man-in-the-Middle attack and how can it be prevented?
- What are the most common application security flaws?
- Describe an experience where you managed or responded to an information security threat or incident. What was the process followed and outcome?
- What are some federal information security laws that would be applicable to the State? How do you keep up with changes to these policies?

Level II and Above

- Provide an example where you analyzed a network attack and defined a risk mitigation strategy. What was the outcome?
- What is your experience with information security standards? Please provide the standards that you use most frequently.
- What are the key components of a successful incident response plan? Describe how you would develop this plan.

- Name three information security standards that could be leveraged by State agencies and why?

Level III Only

- Describe the networking protocols and information security related technologies you have employed. What kind of encryption, firewalls, antivirus software, intrusion prevention systems, and access lists do you recommend?
- How would you lay out a network security infrastructure for an organization concerned about outbound traffic of sensitive information?
- Describe your approach for setting up information security logging and reporting for an organization where highly sensitive data is handled.
- Describe a potential approach to effectively monitor and react to incidents in an organization with millions of daily security events.
- What are some information security trends or best practices that you would be interested in adopting? How do you keep up with new trends and methodologies related to information security?

Information Security Manager[1]

Level I, II, and III

- What is your experience in developing and managing an information security management program?
- What is your experience applying information security principles (e.g. confidentiality, integrity, and availability) to business units?
- How do you tailor program communications to different audiences (e.g., technical, non-technical, across organization levels)?
- What does the ideal information security management program look like (e.g., structure, governance, executive sponsorship, training)? How do you prioritize and delegate responsibilities in developing this program?
- Describe the steps you would take to implement the ISMS program statewide.
- In relation to information security, describe your knowledge of operating systems (e.g., Android, iOS, Linux, Windows, MVS, VMWare), cloud computing, network platforms, and hardware and software platforms.
- Describe an experience where you managed or responded to an information security threat or incident. What was the process and outcome?
- Describe your experience planning and deploying both business and IT related initiatives.
- What are the information security threats you foresee in the near future?
- What is your experience in performing and managing risk or vulnerability assessments? What tools and techniques did you employ?
- Your network has been infected by malware. Please walk me through your mitigation process at a high level.
- What is your understanding of a layered security approach?
- What are the most common application security flaws?
- What are some federal information security laws that would be applicable to the State? How do you keep up with changes to these policies?

Level II and Above

- For an organization where an information security program does not exist, what are the most critical information security initiatives to implement as they relate to:
    - People
    - Process
    - Technology

[1] Inclusive of information technology-related technical questions. Agencies may determine if these questions are applicable to the Information Security Manager position description based on agency need

- What is your experience in identifying and addressing information security and compliance requirements in business functions?
- Describe your experience with enterprise information security and technologies, including but not limited to system and network security, encryption, and authentication.
- Describe your experience managing firewalls, intrusion detection systems, and anti-virus software. What applications did you employ and what do you recommend?
- Describe an approach for the development and implementation of a data classification schema.
- Describe the policies and procedures needed to help ensure compliance with information security policies and procedures.

Level III Only

- What is your experience in managing a team and conveying findings to executive management?
- What is an effective approach to convey the importance of implementing technical security requirements to executive management?
- From the governance perspective, describe an approach to help ensure continuous cooperation between IT, business units, and information security teams.
- Describe your experience in designing, developing, and implementing information security technologies.
- Describe your experience working with network application servers, encryption technologies, and network operation hardware and software.

Information Security and Privacy Auditor

Level I, II, and III

- Describe your knowledge of auditing standards, information security, and privacy compliance frameworks and principles.
- How can these frameworks be applied during the execution of an audit?
- Describe how you would reconcile requirements between auditing, information security, and privacy frameworks to identify the “gold standard”.
- What are some potential vulnerabilities and deviations from standard information security and privacy practices?
- What principles, methods, and tools could be used to evaluate information security and privacy risks? Have you employed these methods in practice? If so, what was the result?
- What is your understanding of a layered security approach?
- What is your understanding of information security standards and regulations which might be applicable to the State (e.g. NIST 800-53, IRS1075, PCI, HITRUST, HITECH)?
- What are some federal information security and privacy laws that would be applicable to the State? How do you keep up with changes to these policies?
- How do you tailor program communications to different audiences (e.g., technical, non-technical, across organization levels)?

Level II and Above

- Describe your experience evaluating information security and privacy controls to help ensure compliance with information security and privacy regulations.
- How do you identify sensitive data in large environments to be able to properly audit for information security and privacy controls?
- What are the most common misconceptions about the information security and privacy functions? How does the information security and privacy functions assist organizations?

Level III Only

- What steps would you take to develop and implement information security and privacy policies and procedures?
- What information security and privacy business and IT / application controls should an organization employ?
- Describe your experience developing information security and privacy audit programs.

- Describe a methodology you have used to report findings to executive management.
- What are some information security and privacy trends or best practices that you would be interested in adopting? How do you keep up with new trends and methodologies related to information security and privacy?

GRC Manager

Level I, II, and III

- What is your experience in developing and managing a GRC program? What policies, training, standards, procedures, technologies, and controls did you employ?
- What processes to do you use to assess, monitor, and report risk?
- Describe your experience working with GRC platforms.
- How do you survey an organization's compliance and regulatory landscape?
- What are some of the success criteria and metrics that you would consider for a successful GRC program and how would you prioritize them?
- How do you define and gather business requirements from business functions/end users and work with the InfoSec and Privacy teams to translate them into functional requirements for implementation into a GRC platform?
- How do changes in requirements and market trends impact GRC processes and technology? What is your process to manage these changes?
- What are the latest information security and privacy threats you foresee for the near future?
- What are some federal information security and privacy laws that would be applicable to the State? How do you keep up with changes to these policies?
- How do you tailor program communications to different audiences (e.g., technical, non-technical, across organization levels)?